ABSTRACT

There is disclosed a high-performance Booth-encoded Montgomery module for performing the computation of A * B * r^{-1} (mod N). A Booth encoder is provided for receiving two bits of A to perform a Booth encoding process, so as to produce a Booth code. A multiplicand selector is provided for receiving B and the Booth code so as to select a multiplicand. A first carry propagate adder is provided for adding the output of the multiplicand selector and a previous computation result to output. A multiplexer is provided for receiving four inputs 0, N, 2N, and 3N from a lookup table and selecting one of the inputs to output. A second carry propagate adder is provided for adding the outputs of the first carry propagate adder and the multiplexer to output. A shifter is provided for shifting the output from the second carry propagate adder to right by two bits, so as to produce a computation result.